UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* A GOLD APPLE IPHONE XR IN A YELLOW AND BLACK "SUPREME" PROTECTIVE COVER; AND A GRAY ALCATEL CELL PHONE CELL PHONE MODEL A405DL	)	Case No.21-mj-392

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. Section 841(a)(1)	Distribution of controlled substances

The application is based on these facts:

See the attached Affidavit in Support of an Application for a Search Warrant.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Kyle Raguz

Applicant's signature

Kyle Raguz- Special Agent, ATF

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/09/2021

/s/ Lynne A. Sitarski

Judge's signature

City and state: _____

Lynne A. Sitarski, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF ONE GOLD APPLE IPHONE XR IN A YELLOW AND BLACK "SUPREME" PROTECTIVE COVER; AND ONE GRAY ALCATEL CELL PHONE MODEL A405DL IMEI 015750001498529 BOTH IN CUSTODY OF ATF LOCATED AT 200 CHESTNUT STREET SUITE 607 PHILADELPHIA, PENNSYLVANIA 19106	Case No. 21-MJ-392

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Kyle Raguz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been since November 2015. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am a graduate of the Criminal Investigator Training Program and the Special Agent Basic Training Program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I am currently assigned to a specialized enforcement group, the ATF Violent Crimes Task Force, whose primary mission is to investigate those individuals and groups that are

engaged in the commission of federal firearms and narcotics violations. I have personally conducted, and assisted in, multiple narcotics investigations into Drug Trafficking Organizations (DTO's). As part of these investigations, I have handled Confidential Informants (CI's), observed and handled heroin, cocaine, crack-cocaine, methamphetamine, and marijuana, and authored and executed multiple search and arrest warrants.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched are One (1) Gold Apple iPhone XR in a Yellow and Black "Supreme" protective cover (hereinafter "SUBJECT DEVICE 1"); and One (1) Gray Alcatel Cell Phone Model A405DL IMEI 015750001498529 (hereinafter "SUBJECT DEVICE 2"). The Devices are currently located at the ATF Philadelphia Field Office at 200 Chestnut Street Suite 607, Philadelphia, Pennsylvania 19106.

5. The applied-for warrant would authorize the forensic examination of the Device's for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The ATF and Philadelphia Police Department ("PPD") are investigating a Drug Trafficking Organization (DTO) that operates on and around the 1700 block of Brill Street in Philadelphia, PA. Members of this DTO include Kelvin JIMENEZ a/k/a "Nip" (JIMINEZ), Jason CLARK a/k/a "Rock" (CLARK), and others known and unknown. The violations include, inter alia, 21 U.S.C. § 841(a)(1) (distribution of controlled substances).

7. In June of 2019, ATF Special Agent Kyle Raguz and PPD Detective Justin Falcone interviewed a confidential source, herein referred to as CS-1. CS-1 has cooperated with

investigators in the past and has provided reliable and accurate information. CS-1's assistance has led to multiple successful Federal investigations. CS-1 has, in the past, made statements against his/her own penal interest. The information provided by CS-1 in connection with the current investigation has been corroborated by surveillance, police reports, witness interviews, Department of Motor Vehicle records, law enforcement databases, telephone records, information gathered from social media and controlled purchases of illicit narcotics. CS-1 is currently a registered confidential informant with ATF, who is being paid in connection with his/her work in this investigation. CS-1 has no pending criminal cases and is not receiving any judicial consideration in connection with his/her cooperation. In June of 2019, ATF agents instructed CS-1 to go to the area of Brill Street and Charles Street in Philadelphia, PA to narcotics dealers. Investigators knew this area to be a high crime area where two Drug Trafficking Organizations ("DTO's") were competing for territory, resulting in multiple reports of violent crimes to include assaults, shootings, and homicides.

8. On or about June 27, 2019, ATF GROUP VI instructed CS-1 to travel to the 1700 block of Brill Street in Philadelphia to make contact with narcotics traffickers in the area. CS-1 made contact with CLARK at the corner of Brill and Charles Streets in Philadelphia and conducted a controlled purchase of approximately 17 grams of marijuana, all monitored by electronic audio and video recording equipment. CS-1 was searched for money and contraband before and after the controlled purchase with negative results. During the controlled purchase, CLARK introduced himself as "Rock" and provided his telephone number, 267-647-8145, to CS-1 for future narcotics purchases. The alleged marijuana purchased by CS-1 from CLARK was brought back to the ATF office for processing, where a field test yielded a positive result of the presence of marijuana. The

drugs were sent to the Philadelphia Police Department Laboratory for further analysis, which confirmed the substance was marijuana.

9. On or about July 8, 2019, Special Agent Raguz and Philadelphia Police Department Detective Justin Falcone recorded a consensual phone call from CS-1 to CLARK that occurred over the number CLARK previously provided to CS-1. The conversation included details for an illicit narcotics transaction to occur on July 10, 2019. On or about July 10, 2019 ATF Group VI utilized CS-1 to conduct a controlled purchase of approximately 17.8 grams of marijuana and 7.8 grams of cocaine from CLARK, all monitored by electronic audio and video recording equipment. CS-1 was searched for money and contraband before and after the controlled purchase with negative results. The alleged marijuana and cocaine purchased by CS-1 from CLARK was brought back to the ATF office in for processing, where a field test yielded a positive result for the presence of cocaine. The drugs were sent to the Philadelphia Police Department Laboratory for further analysis, which confirmed the substances were marijuana and cocaine.

10. On or about July 15, 2019, Special Agent Raguz and PPD Detective Falcone recorded a consensual phone call from CS-1 to CLARK that occurred over the number CLARK previously provided to CS-1. The conversation included details for an illicit narcotics transaction to occur on the following day. On or about July 16, 2019, ATF Group VI utilized CS-1 to conduct a controlled purchase of approximately 39.4 grams of "crack" cocaine from CLARK. CS-1 was searched for money and contraband before the controlled purchase with negative results. The transaction was monitored by electronic audio and video recording equipment, and occurred at the intersection of Brill Street and Charles Street in Philadelphia, PA. Following the meeting with CLARK, CS-1 returned to the agents, again was searched, and provided agents with a sum of cocaine that CS-1 had purchased from CLARK. The alleged "crack" cocaine was brought back to

the ATF office in Philadelphia for processing, where a field test yielded a positive result for the presence of cocaine. The drugs were sent to the Philadelphia Police Department laboratory for further analysis, which confirmed the substance was cocaine base with a weight of approximately 39.4 grams.

11. On or about August 6, 2019, Special Agent Raguz and PPD Detective Falcone recorded a consensual phone call from CS-1 to CLARK, which occurred over the telephone number CLARK previously provided to CS-1. The conversation included details for an illicit narcotics transaction to occur on the following day. On or about August 7, 2019, ATF Group VI utilized CS-1 to conduct a controlled purchase of approximately 51.98 grams of "crack" cocaine from CLARK near 5400 Erdrick Street in Philadelphia. CS-1 was searched for money and contraband before the controlled purchase with negative results, and was monitored by electronic audio and video recording equipment. Following the meeting with CLARK, CS-1 returned to the agents, again was searched, and provided agents with a sum of "crack" cocaine that CS-1 had purchased from CLARK. The alleged cocaine was brought back to the ATF office in Philadelphia for processing, where a field test yielded a positive result for the presence of cocaine. The drugs were sent to the Philadelphia Police Department Laboratory for additional analysis, which confirmed the presence of cocaine base in two separate bags with a combined weight of 51.98 grams.

12. On or about August 19, 2019, Special Agent Raguz recorded a consensual phone call from CS-1 to CLARK, which occurred over the telephone number CLARK previously provided to CS-1. The conversation included details for an illicit narcotics transaction to occur on the following day. On or about August 22, 2019, ATF Group VI utilized CS-1 to conduct a controlled purchase of approximately 29 grams of "crack" cocaine and 7.8 grams of marijuana

from CLARK near 5400 Erdrick Street in Philadelphia. CS-1 was searched for money and contraband before the controlled purchase with negative results, and was monitored by electronic audio and video recording equipment. Following the meeting with CLARK, CS-1 returned to the agents, again was searched, and provided agents with a sum of crack cocaine and marijuana that CS-1 had purchased from CLARK. The alleged cocaine was brought back to the ATF office in Philadelphia for processing, where a field test yielded a positive result for the presence of cocaine and marijuana. The drugs were sent to the Philadelphia Police Department laboratory for further analysis, which confirmed that the alleged crack cocaine was in fact cocaine base with a weight of 24.8 grams. The alleged marijuana was confirmed to be marijuana with a weight of 3.2 grams.

13. On October 20, 2020, CS-1 approached several males on the 1700 block of Brill Street near Charles Street and stated he was interested in buying narcotics. CS-1 stated he knew "Nip" (JIMENEZ) and "Rock" (CLARK). CS-1 stated that someone on the block, later identified by investigators as Steven TORRES, attempted to contact JIMENEZ and CLARK on a cellular telephone. After JIMENEZ failed to answer, TORRES called CLARK. CS-1 was able to overhear a portion of the conversation between TORRES and CLARK and heard CLARK say that he knew CS-1 but did not have anything to sell that day.

14. On November 4, 2020, CLARK was charged by a Federal Grand Jury in the Eastern District of Pennsylvania for the above-described controlled purchases. Specifically, he was charged with one (1) count of distribution of marijuana in violation of 21 U.S.C. § 841(a)(1), (b)(1)(D), one (1) count of distribution of cocaine and marijuana in violation of 21 U.S.C. § 841(a)(1), (b)(1)(C), (b)(1)(D), two (2) counts of distribution of 28 grams or more of cocaine base ("crack") in violation of 21 U.S.C. § 841(a)(1), (b)(1)(B) and one (1) count of distribution of cocaine base ("crack") and marijuana in violation of 21 U.S.C. § 841(a)(1), (b)(1)(C), (b)(1)(D).

On December 8, 2020, ATF Group VI Task Force members executed the arrest warrant associated with this indictment by taking CLARK into custody as he was walking along the 3200 block of Saint Vincent Street in Philadelphia, Pennsylvania. Recovered from his person were two cell phones, SUBJECT DEVICES 1 and 2.

15. Based on my training and experience, I know that cellular telephones can be tampered with or erased remotely while connected to a cellular network. Based on this knowledge, upon seizing the SUBJECT DEVICES, investigators placed the SUBJECT DEVICES into airplane mode or power down mode to disconnect them from the cellular network to prevent destruction of evidence. On March 2, 2021, investigators attempted to dial the known phone number, 267-647-8145, for CLARK to see if either of the SUBJECT DEVICES rang, but due to the lack of connectivity to a cellular network, agents were unable to determine whether either of the SUBJECT DEVICES are assigned the aforementioned phone number. Notably, no one answered the phone when investigators dialed the known phone number.

16. Investigators believe, regardless if whether the known number matches the SUBJECT DEVICES, that the SUBJECT DEVICES contain communications relating to the offenses under investigation. Investigators have recorded multiple consensual calls between CS-1 and CLARK who was using at the time the following phone number: 267-647-8145. Those phone calls included discussions regarding scheduling and executing narcotics transactions between CS-1 and CLARK. Based on my training and experience described in greater detail below, I believe that a search of the contents of SUBJECT DEVICES 1 and 2 will reveal additional valuable information about CLARK's drug trafficking activities, associates, and methods of operation.

17. Based on my training and experience, I know that individuals involved in drug trafficking often maintain more than one phone in order to have multiple avenues to facilitate drug trafficking activities, and in an attempt to avoid detection by law enforcement. I am aware that individuals involved in drug trafficking often times utilize pre-paid cellular telephones which do not maintain specific subscriber information, and/or use phones subscribed to in the name of third person, in order to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. Further, those involved in drug trafficking often change phones and phone numbers in order to make it difficult for law enforcement to determine their records. Based on my training and experience, I know that individuals involved in drug trafficking also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, drug traffickers often keep old phones.

18. Based on my training and experience, I know that drug traffickers commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, I know that drug traffickers often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

19. Specifically, I know that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know those involved in drug trafficking communicate with associates using cellular telephones

and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

20. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific traffickers.

21. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. I am also aware that drug traffickers often take photographs or make videos of drugs and drug proceeds with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

22. Furthermore, based on my training and experience and the training and experience of other agents, I know that drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use an Internet search engine to explore where banks or mail delivery services are located, or may use the Internet to make reservations for drug-related travel. In addition, I know that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order

to communicate with co-conspirators, and to display drugs and drug proceeds or to post photographs of locations where they have traveled in furtherance of their drug trafficking activities.

23. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

24. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other

digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs

usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, I know that the SUBJECT DEVICES listed in Attachment A have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Additionally, the SUBJECT DEVICES may contain call logs, address books, text messages, emails, videos, photographs, or other stored data relevant to this investigation.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31. For the reasons set forth above, I believe there is probable cause to search SUBJECT DEVICE 1 and SUBJECT DEVICE 2 in Attachment A for evidence of violations of 21 U.S.C. § 841(a)(1). I believe there is probable cause to conduct a search of the SUBJECT DEVICES consistent with Attachment B which permits a search of all stored data to include, but not limited to contents of the telephone directory, electronic libraries, stored communications including voice mail, voice messages and text messages, contact lists, applications, reference material aiding in the furtherance of criminal activity, photographs, time and date stamps, Global Positioning System (GPS) data, stored internet searches and any other memory feature relating to the offenses outlined in the affidavit of probable cause.

Respectfully submitted,

/s/ Kyle M. Raguz

Kyle M. Raguz, Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

Subscribed and sworn to before me
on March 9, 2021:

/s/ Lynne A. Sitarski

HONORABLE LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE
Eastern District of Pennsylvania

ATTACHMENT A

The property to be searched are the cellular telephones that are listed below:

a. One (1) Gold /Yellow Apple iPhone XR in a Yellow and Black "Supreme" protective cover and

b. One (1) Gray Alcatel Cell Phone Model A405DL IMEI 015750001498529

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

The Devices are currently located at the ATF Philadelphia Field Office at 200 Chestnut Street Suite 607, Philadelphia, Pennsylvania 19106.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the SUBJECT DEVICE described in Attachment A that relate to violations of title 21, United States Code, Section 841(a)(1) and involve CLARK, including:

1. Contents of the telephone directory;

2. Electronic libraries;

3. Stored communications including voice mail, voice messages and text messages, contact lists, applications, reference material aiding in the furtherance of criminal activity;

4. Photographs;

5. Videos;

6. Time and date stamps;

7. Global Positioning System (GPS) data;

8. Stored internet searches;

9. Any other memory feature relating to the offenses outlined in the affidavit of probable cause.

10. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.